CLAIMS

We claim:

1. A method of operating an intrusion detection system, the method comprising the steps of:

taking a base action in response to detecting an intrusion;

updating an action counter in response to taking the base action;

comparing the value of the action counter to an action threshold;

updating an action variable when the value of the action counter meets the action threshold;

checking a validity condition for satisfaction dependent upon the action variable; and

invoking a provision associated with the validity condition when the validity condition is satisfied.

2. The method of claim 1, wherein the provision changes an element of a base intrusion set.

3. The method of claim 2, wherein the element of the base intrusion set is a signature event.

4. The method of claim 2, wherein the element of the base intrusion set is a signature event counter.

5. The method of claim 2, wherein the element of the base intrusion set is a signature threshold.

6. The method of claim 2, wherein the element of the base intrusion set is a base action.

7. The method of claim 2, wherein the element of the base intrusion set is a weight.

8. The method of claim 1, wherein the provision changes an element of an action set.

9. The method of claim 8, wherein the element of the action set is an action counter.

10. The method of claim 8, wherein the element of the action set is an action threshold.

11. The method of claim 8, wherein the element of the action set is an action variable.

12. A method of operating an intrusion detection system, the method comprising the steps of:

detecting a signature event;

updating a signature event counter responsive to detecting the signature event;

comparing the value of the signature event counter to a signature threshold;

updating an action counter when the value of the signature event counter meets the signature threshold;

comparing the value of the action counter to an action threshold;

updating an action variable when the value of the action counter meets the action threshold;

checking a validity condition for satisfaction dependent upon the action variable; and

invoking a provision associated with the validity condition when the validity condition is satisfied.

13. The method of claim 12, wherein the provision changes an element of a base intrusion set.

14. The method of claim 13, wherein the element of the base intrusion set is a signature event.

15. The method of claim 13, wherein the element of the base intrusion set is a signature event counter.

16. The method of claim 13, wherein the element of the base intrusion set is a signature threshold.

17. The method of claim 13, wherein the element of the base intrusion set is a base action.

18. The method of claim 13, wherein the element of the base intrusion set is a weight.

19. The method of claim 12, wherein the provision changes an element of an action set.

20. The method of claim 19, wherein the element of the action set is an action counter.

21. The method of claim 19, wherein the element of the action set is an action threshold.

22. The method of claim 19, wherein the element of the action set is an action variable.